Exhibit A

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION**

JOSEPH VAN LOON; TYLER ALMEIDA; ALEXANDER FISHER; PRESTON VAN LOON; KEVIN VITALE; and NATE WELCH,	))))	
Plaintiffs,	)))	
v.	))	No. 1:23-cv-00312-RP
DEPARTMENT OF THE TREASURY; OFFICE OF FOREIGN ASSETS CONTROL; JANET YELLEN, in her official capacity as Secretary of the Treasury; and ANDREA M. GACKI, in her official capacity as Director of the Office of Foreign Assets Control,	))))))))	
Defendants.	)	

**BRIEF OF AMICUS CURIAE PARADIGM OPERATIONS LP
IN SUPPORT OF PLAINTIFFS'
MOTION FOR PARTIAL SUMMARY JUDGMENT**

CORPORATE DISCLOSURE STATEMENT

Paradigm Operations LP ("Paradigm") discloses the following information for the limited purpose of complying with Rule 7.1(a)(1) of the Federal Rules of Civil Procedure. Paradigm has no parent corporation. No publicly held corporation owns 10% or more of Paradigm's stock.

Paradigm reserves the right to supplement this disclosure statement if needed.

TABLE OF CONTENTS

Page(s)

TABLE OF AUTHORITIES

INTEREST OF AMICUS CURIAE

Paradigm Operations LP ("Paradigm") is an investment firm that backs innovative crypto companies and protocols. Paradigm seeks leave to participate in this case because it is concerned that the Department of Treasury's ("the Department") unprecedented sanctioning of publicly available software is an unfounded expansion of sanctions law that far exceeds the Department's statutory authority and would deprive law-abiding Americans of a critical privacy tool. Moreover, the novel argument the Department puts forward to justify its regulation of technology— essentially that developers and users of Tornado Cash form some sort of unincorporated entity— is itself a broad and far-reaching theory that would effectively conscript unwitting coders and technology users into becoming members of a legal entity not of their choosing and, as a result, inhibit the viability of open-source software development in the United States.

INTRODUCTION

Blockchain technology is an emerging computing paradigm that, while still in its early stages of development, has made peer-to-peer digital payments possible and is enabling new forms of human coordination and more complex applications that are colloquially referred to as "Web3." Blockchains are at their core computer networks that enable a decentralized set of unaffiliated "nodes" to maintain a shared database. One of blockchain technology's defining features is that this shared database or "ledger" is completely transparent: anyone can view all of the information dating back to the first transaction.

A blockchain's transparency provides an important safety measure since it allows anyone to audit the data. However, it can also raise alarming privacy concerns for users. While a blockchain user's address is pseudonymous, if linked to a real-world identity (which happens), it could expose that user's complete history, including sensitive transactions or affiliations, and make

them the target of bad actors. In practice, this is akin to publishing one's entire history of bank account statements or credit card bills for anyone to see online. Moreover, as blockchain adoption increases and more users rely on blockchain infrastructure for online financial and social interactions, these privacy concerns will only increase.

Tornado Cash is a publicly available software, a tool or application, that was designed to address these privacy concerns and enable Ethereum users to shield their information. In practice, Tornado Cash attempts only to provide users of Ethereum a similar level of privacy that we have come to expect of our existing financial transactions. The core Tornado Cash tools are "pools," which refer to applications enabled by smart contracts deployed to the Ethereum blockchain that allow users to deposit tokens from one address and later withdraw those same tokens to a different address on the Ethereum network.[1] While a user's deposit or withdrawal from a Tornado Cash pool is publicly broadcast on the Ethereum network, the link between the deposit and withdrawal addresses is broken. Tornado Cash, therefore, acts as a type of "private changing room" that provides the withdrawal address with some level of privacy because it cannot easily be linked to the deposit address. The level of privacy increases as the relevant pool has more volume.

The smart contracts for the relevant Tornado Cash pools are "immutable"—that is, no one can control, update, or remove them from the Ethereum network. In addition, Tornado Cash pools

---

[1] "When developers program smart contracts, they decide what operations the smart contract will support and what rules those operations must follow. These rules and operations are written using code that is broadcast to Ethereum's network, just like the token transactions described above. Once a smart contract's code is added to Ethereum's records, it receives a unique address and can be interacted with by any user to automatically carry out the rules and operations it supports. In essence, smart contracts are open-source applications that anyone can deploy to Ethereum. Just like the rest of Ethereum, smart contracts can be viewed and used by anyone, anywhere, and without relying on an intermediary." *How does Tornado Cash Work?* Coincenter (Aug. 25, 2022), https://bit.ly/3KZwBUy.

are entirely "non-custodial," meaning that at no point is a user who deposits tokens into the pool required to relinquish control of those tokens.

When Tornado Cash is properly conceptualized as an array of publicly available software applications—*i.e.*, code—that cannot be owned, updated, or removed and that do not take control of users' assets, it is clear that "Tornado Cash" is not a legal person that should be subject to sanctions.[2] However, in a gambit to expand its authority to regulate technology, the Department argues that "Tornado Cash" is an undefined type of "entity." *Treasury Designates DPRK Weapons Representative*, Department of Treasury (Nov. 8, 2022), https://bit.ly/3UORTHP. But in fact, Tornado Cash is just open-source code:

```
/**
 *Submitted for verification at Etherscan.io on 2019-12-16
*/

// File: contracts/MerkleTreeWithHistory.sol

// https://tornado.cash
/*
* d888888P                                                dP          a88888b.              dP
*    88                                                   88         d8'   `88              88
*    88    .d8888b. 88d888b. 88d888b. .d8888b. .d888b88 .d8888b.     88        .d8888b. .d8888b. 88d888b.
*    88    88'  `88 88'  `88 88'  `88 88'  `88 88'  `88  88        88'  `88 Y8ooooo. 88'  `88
*    88    88.  .88 88       88 88.  .88 88.  .88 .88 dP Y8.       .88 88.  .88        88 88       88
*    dP    `88888P' dP       dP dP `88888P8 `88888P8 `88888P' 88 Y88888P' `88888P8 `88888P' dP       dP
* oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo
*/

pragma solidity ^0.5.8;

library Hasher {
  function MiMCSponge(uint256 in_xL, uint256 in_xR) public pure returns (uint256 xL, uint256 xR);
}

contract MerkleTreeWithHistory {
  uint256 public constant FIELD_SIZE =
21888242871839275222246405745257275088548364400416034343698204186575808495617;
  uint256 public constant ZERO_VALUE =
21663839004416932945382355908787605992252266501822290791145750497851557825542129; // = keccak256("tornado") %
FIELD_SIZE
```

---

[2] There are centralized businesses that offer "mixing" services, such Blender.io, which have also been the subject of sanctions by the Department. *U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats*, Department of Treasury (May 6, 2022), https://bit.ly/41rOCQI. In stark contrast to Tornado Cash, mixers like Blender.io work by requiring users to relinquish their tokens to a centralized business entity, which will exercise control over those tokens and subsequently return them to the user for a fee.

Tornado Cash Contract Source Code, Etherscan (accessed Apr. 14, 2023), https://bit.ly/41fprkz.

The Department therefore has no authority to sanction Tornado Cash and this Court should grant

the Plaintiffs' Motion for Partial Summary Judgment.

ARGUMENT

I.   The Department's authority is limited to blocking "property" of "persons."

The Department sanctioned Tornado Cash pursuant to Executive Orders (E.O.) 13694 and

13722. Broadly, E.O. 13694 issued by President Barack Obama in April 2015 "block[s]" and

prohibits the transfer or dealing of "[a]ll property and interests in property" of "any person" the

Department has determined to have engaged in "significant malicious cyber-enabled activities."

E.O. No. 13694, 80 Fed. Reg. 18,077 (Apr. 1, 2015). E.O. 13722, issued by President Obama in

March 2016, "block[s]" and prohibits the transfer or dealing of "[a]ll property and interests in

property" of the North Korean government within the United States or in the control of a United

States person or of "any person" who generally conducts or has conducted business with the North

Korean government. E.O. No. 13722, 82 Fed. Reg. 17,331 (Mar. 15, 2016). Each E.O. is limited

to apply only to "property" or "interests in property" "that are in the United States, that hereafter

come within the United States, or that are or hereafter come within the possession or control of

any United States person." E.O. 13694; E.O. 13722.

Of course, "an agency literally has no power to act . . . unless and until Congress confers

power upon it." *Louisiana Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 374 (1986). Both E.O.s

13694 and 13722 were issued, in part, pursuant to the International Emergency Economic Powers

Act (IEEPA), which permits the President "under such regulations as he may prescribe" to:

> investigate, block during the pendency of an investigation, regulate, direct and
> compel, nullify, void, prevent or prohibit, any acquisition, holding, withholding,
> use, transfer, withdrawal, transportation, importation or exportation of, or dealing
> in, or exercising any right, power, or privilege with respect to, or transactions

involving, any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United States.

50 U.S.C. § 1702(a)(1)(B). E.O. 13722 was also issued, in part, pursuant to the North Korea

Sanctions and Policy Enhancement Act of 2016, which permits the president to "designate . . . any

person" the President determines has knowingly assisted or engaged in commerce with the North

Korean government. 22 U.S.C. § 9214(a).

As explained in Plaintiffs' Motion for Partial Summary Judgment, the Department's own

regulations clearly define "person," "property," and "interest." Dkt. No. 41 at 16-17. In brief,

"property" and "property interest" are assets, tangible or intangible, that are capable of being

owned. *See* 31 C.F.R. § 510.323. And under the Department's designation and regulations, a

"person" includes an "individual or "entity," with an entity defined as "a partnership, association,

trust, joint venture, corporation, group, subgroup, or other organization." 31 C.F.R. §§ 510.322;

510.305. Although IEEPA, the Department's own regulations, and the E.O.s do not further define

"a partnership, association, trust, joint venture, corporation, group, subgroup, or other

organization," *id.*, dictionary definitions confirm that an "entity" generally means a group of

individuals that intend to work toward a common purpose.[3] *See also* Pls.' Mot. for Partial Summ.

---

[3] **Partnership**: "A voluntary association of two or more persons who jointly own and carry on a business for profit." Black's Law Dictionary (11th ed. 2019).
Association: "A gathering of people for a common purpose; the persons so joined." *Id.*
Joint Venture: "A business undertaking by two or more persons engaged in a single defined project. The necessary elements are (1) an express or implied agreement; (2) a common purpose that the group intends to carry out; (3) shared profits and losses; and (4) each member's equal voice in controlling the project." *Id.*
Corporation: "An entity (usu. a business) having authority under law to act as a single person distinct from the shareholders who own it and having rights to issue stock and exist indefinitely; a group or succession of persons established in accordance with legal rules into a legal or juristic person that has a legal personality distinct from the natural persons who make it up, exists indefinitely apart from them, and has the legal powers that its constitution gives it." *Id.*

J., Dkt. No. 41 at 19 (arguing that status as unincorporated entity defined by agreement to "pursue a common purpose."). Accordingly, for parties to form an unincorporated association or legal entity, there must be an *intent* to work toward a common purpose. There is no evidence that Tornado Cash, its founders, code developers, or the diffuse number of individuals holding Tornado Cash "TORN" digital tokens have ever intended to work toward a common purpose and form an unincorporated association. As a result, the Department's sanctions clearly exceed its statutory authority.

II.   **Tornado Cash is neither property nor a person or otherwise an entity that the Department has authority to sanction.**

Here, there is no debate that Tornado Cash is not "property" or "property interest," 31 C.F.R. § 510.323, since immutable smart contracts based on open-source software cannot be controlled or owned. But the Department has stated that the "person" it has sanctioned is "the entity known as Tornado Cash, which is a partnership, association, joint venture, corporation, group, subgroup, or other organization." Office of Foreign Asset Control, FAQ 1095 (Nov. 8, 2022), https://bit.ly/3KMRx0C [hereinafter "FAQ 1095"]. Notably, the Department has not specified which *type* of entity Tornado Cash is, opting instead to simply refer to the full regulatory definition of "entity." 31 C.F.R. §§ 510.305, 578.305.

The Department's theory for sanctioning Tornado Cash is that Tornado Cash is a Frankenstein-like creature, assembled from disparate components that, when combined, become a legal person. Peter Van Valkenburgh, *Tornado Cash is no "golem." It's a tool for privacy and free speech*, CoinCenter (Oct. 26, 2022), https://bit.ly/3o8lZJL. According to the Department, the

---

Group: "A number of individuals assembled together or having some unifying relationship." Merriam-Webster (2023).
Organization: "A group that has formed for a particular purpose." Black's Law Dictionary (11th ed. 2019).

Tornado Cash "organizational structure" consists of: (1) unnamed "founders and other associated developers" and (2) "the Tornado Cash [Decentralized Autonomous Organization] DAO. . . ." FAQ 1095.[4] This latter group includes thousands of wallet addresses holding Tornado Cash's digital tokens known as "TORN." Tornado Cash, CoinMarketCap (accessed Apr. 14, 2023), https://bit.ly/3KMr6YZ. Not all TORN token holders vote, and none has any control over the Tornado Cash pools. However, the Department's novel theory that Tornado Cash is an entity because it consists of unnamed founders, developers, and TORN token holders fails because this disparate mix of actors have wide ranging levels of involvement in the project, including no involvement at all, may hold the asset for different reasons, and have potentially conflicting motivations and incentives. As a result, they collectively lack the level of coordination needed to be considered a unified legal entity.

In an apparent bid to hedge its position and avoid directly sanctioning any individual, the Department simultaneously noted in FAQ 1095 that it "has not designated Tornado Cash's individual founders, developers, members of the DAO, or users, or other persons involved in supporting Tornado Cash at this time." FAQ 1095. The Department's resulting incoherent position is that it has sanctioned a fictional entity, of an unspecified type, composed of members who are themselves exempt from that same sanction. The Department's blatant avoidance of designating any actual person associated with Tornado Cash demonstrates how it has gone beyond its statutory authority to sanction technology rather than an actual person or entity. To be clear, the Department

---

[4] Fundamentally, DAOs are a way to organize people, a social-coordination technology that relies on blockchain-based smart contracts and incentives to facilitate individuals collaborating and taking actions with collective impact. DAOs enable new communities to form and collaborate on shared goals by providing increased "transparency, trust, adaptability and speed" in making decisions as compared to traditional decision-making approaches. David Gogel et al., *Decentralized Autonomous Organizations: Beyond the Hype*, World Econ. F., 4–5 (June 2022), https://bit.ly/3KvLFaU.

also did not rule out the authority to sanction all those persons, including TORN token holders who may have unintentionally received one. So, where liability could fall in the future is unclear.

Nothing in the record suggests that Tornado Cash's unnamed founders and associated developers have intended to work toward a common purpose, nor do they have any power or control over the immutable Tornado Cash pools. The publicly available Tornado Cash codebase has 11 individual contributors, including presumably some of the unnamed founders. Tornadocash, Github (accessed Apr. 14, 2023), https://bit.ly/3o9FmlO. The Tornado Cash code builds upon existing open-source code and incorporates dependencies[5] that themselves are the product of contributions from many thousands of unaffiliated developers over many years. Read literally, the Department's statement that Tornado Cash is an unincorporated entity partially made up of "founders and associated developers" could be interpreted to encompass even developers that have only contributed code indirectly. FAQ 1095. The Department has not delineated exactly which of these contributors are supposedly part of the unincorporated association, nor has it shown they have intended to work toward a common purpose. This Court should make clear that developers do not get conscripted into a legal entity when they suggest a revision to publicly available code, or have their existing code integrated into a new codebase. In short, people do not become part of a putative unincorporated association merely because they interact with software.

As for the Tornado Cash DAO, that is not an entity because it is an amalgamation of all TORN owners. Some, but not all, of whom may vote on certain governance related proposals created by developers. But merely voting on these proposals does not mean that TORN token holders have intended to work toward a common purpose, and it is clearly not enough to create an

---

[5] In the context of software development, a "dependency" is a relationship between software components where one component relies on the other to work properly. For example, if a software application uses a library to query a database, the application depends on that library.

unincorporated association. In addition, the Department's description of TORN token holders is inaccurate. Token holders are not required or "responsible" for voting, *contra* FAQ 1095, which is completely voluntary and in practice has extremely low participation. A person can purchase tokens, simply hold them, and never choose to vote on anything. Alternatively, a TORN holder may participate in one vote and then sell tokens without interacting with Tornado Cash again or delegate voting rights to others. More importantly, token holders are not "voting on and implementing new features" as they relate to the core Tornado Cash privacy tool because the Tornado Cash smart contract "pools" are all immutable, and so TORN token holders have no power to change them.

III.   The Department's theory for sanctioning Tornado Cash is unprecedented and far-reaching.

The Department's theory for sanctioning Tornado Cash implies that unassociated developers can become part of an "entity" simply because they have contributed code, knowingly or unknowingly, to a blockchain protocol. Blockchain-enabled communities, in particular DAOs, have taken shape in ways that do not conform to existing corporate entities, such as corporations or limited liability companies. *Cf.* Chris Brummer and Rodrigo Seira, *Legal Wrappers and DAOs* (July 7, 2022), https://bit.ly/43vD8xi. As a result of the mismatch between blockchain-enabled communities and recognized legal entities, the potential liability of various participants in these communities is an open question that is being litigated in various regulatory and civil actions. Although the Department's theory for sanctioning Tornado Cash here is fundamentally that disparate unaffiliated individuals can form an unincorporated entity capable of being sanctioned, it implies that the Department could, if it wanted, go after code developers who have contributed to open-source publicly available codes like Tornado Cash merely because of their contribution to that code.

9

This is a slippery slope—implying that code developers can unwittingly be roped into sanctions through their code contributions. And it goes beyond the liability theories other agencies have relied upon. For instance, in the first regulatory enforcement action involving a DAO, the Commodity Futures Trading Commission (CFTC) merely argued that the "Ooki DAO"—another blockchain protocol—was an unincorporated general partnership comprised of token holders who actually voted. *See CFTC v. Ooki DAO*, No. 3:22-cv-05416-WHO (N.D. Cal.). Although the CFTC's position that this DAO is an unincorporated general partnership is wrong, the Department's position in this case goes even further—implying that *all* TORN token holders *plus* Tornado Cash's founders and associated developers can form an unincorporated entity.

Moreover, the Department's attempt to conscript developers and token holders into joining a Frankenstein unincorporated association could imperil the viability of open-source code development in the United States. Open-source code is the backbone of today's technological stack, and the product of countless contributions from individual developers. As an indirect result of this case, these developers could suddenly find themselves at risk of being unwittingly ensnared into joining a legal entity by simply making contributions to open-source code. Indeed, the lack of clarity about what specific test the Department used to determine organizational status and membership is so unclear that it would be difficult for people to know for sure if their activities— which might be as simple as receiving a TORN token unwittingly from another and leaving it in their wallet—could subject them to be considered members of an unincorporated association with devastating legal consequences. Or, consider a developer whose unrelated open-source software contribution to the public domain was used in code development. Could that unknowing contribution trigger membership in an unincorporated association and thus subject him to sanctions?

To avoid inhibiting Americans from freely contributing to the development of publicly available technologies, this Court should be extremely weary of endorsing the Department's theories about the presumed collective legal personhood of individuals interacting with software.

* * *

Essentially, the Department's sanctioning here is a ban on privacy technology like Tornado Cash. Yet there are important, non-nefarious reasons why law-abiding citizens seek to use Tornado Cash to protect their transactions. Today, you can use digital currency for mundane day-to-day transactions like buying a movie ticket or for transactions that reasonable people would want to keep private—paying for a doctor's visit or donating to political or charitable causes. As digital currencies like Ethereum become more established, protecting this privacy will become even more important. After all, the current default is that financial transactions are generally private, and no one expects to see their credit or debit card transactions posted publicly for the world to see and traced back to them. There is no reason why Ethereum users should not be able to avail themselves of the same level of protection and anonymity in their transactions through the use of applications like Tornado Cash. And the Department's unparalleled and expansive use of its authority not only represents a real threat to financial privacy but also to the future of open-source code development and the digital blockchain industry more generally.

CONCLUSION

The Court should grant Plaintiffs' motion for partial summary judgment.

Dated: April 14, 2023

Respectfully submitted,

/s/ Katherine C. Yarger
Katherine C. Yarger*
katie@lehotskykeller.com
LEHOTSKY KELLER LLP
700 Colorado Blvd., #407
Denver, CO 80206

11

(512) 693-8350

Alexis Swartz
alexis@lehotskykeller.com
LEHOTSKY KELLER LLP
919 Congress Avenue
Ste. 1100
Austin, TX 78701
(512) 693-8350

Rodrigo Seira*
rodrigo@paradigm.xyz
PARADIGM OPERATIONS LP
548 Market Street
San Francisco, CA 94104

*Pro Hac Vice Application Pending

CERTIFICATE OF SERVICE

I hereby certify that on April 14, 2023, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notice of electronic filing to all counsel of record who have consented to electronic notification.

/s/ Alexis Swartz
Alexis Swartz